

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Q.3309

(10/2009)

СЕРИЯ Q: КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ

Требования к сигнализации и протоколы СПП –
Протоколы управления ресурсами

Протокол координации QoS

Рекомендация МСЭ-Т Q.3309

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Q
КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ

| | |
|--|----------------------|
| СИГНАЛИЗАЦИЯ ПРИ РУЧНОМ СПОСОБЕ УСТАНОВЛЕНИЯ МЕЖДУНАРОДНЫХ СОЕДИНЕНИЙ | Q.1–Q.3 |
| АВТОМАТИЧЕСКОЕ И ПОЛУАВТОМАТИЧЕСКОЕ МЕЖДУНАРОДНОЕ СОЕДИНЕНИЕ | Q.4–Q.59 |
| ФУНКЦИИ И ИНФОРМАЦИОННЫЕ ПОТОКИ ДЛЯ СЛУЖБ ЦСИС | Q.60–Q.99 |
| СЛУЧАИ, ПРИМЕНИМЫЕ К СТАНДАРТИЗИРОВАННЫМ СИСТЕМАМ МСЭ-Т | Q.100–Q.119 |
| ТРЕБОВАНИЯ К СИСТЕМАМ СИГНАЛИЗАЦИИ № 4, 5, 6, R1 и R2 | Q.120–Q.499 |
| ЦИФРОВЫЕ СТАНЦИИ | Q.500–Q.599 |
| ВЗАИМОДЕЙСТВИЕ СИСТЕМ СИГНАЛИЗАЦИИ | Q.600–Q.699 |
| ТРЕБОВАНИЯ К СИСТЕМЕ СИГНАЛИЗАЦИИ № 7 | Q.700–Q.799 |
| ИНТЕРФЕЙС Q3 | Q.800–Q.849 |
| ЦИФРОВАЯ АБОНЕНТСКАЯ СИСТЕМА СИГНАЛИЗАЦИИ № 1 | Q.850–Q.999 |
| СЕТЬ СУХОПУТНОЙ ПОДВИЖНОЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ | Q.1000–Q.1099 |
| ВЗАИМОДЕЙСТВИЕ СО СПУТНИКОВЫМИ ПОДВИЖНЫМИ СИСТЕМАМИ | Q.1100–Q.1199 |
| ИНТЕЛЛЕКТУАЛЬНАЯ СЕТЬ | Q.1200–Q.1699 |
| ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ IMT-2000 | Q.1700–Q.1799 |
| ХАРАКТЕРИСТИКИ СИГНАЛИЗАЦИИ, ОТНОСЯЩИЕСЯ К УПРАВЛЕНИЮ ВЫЗОВАМИ НЕЗАВИСИМО ОТ КАНАЛА ПЕРЕДАЧИ ДАННЫХ (VICS) | Q.1900–Q.1999 |
| ШИРОКОПОЛОСНАЯ ЦСИС | Q.2000–Q.2999 |
| ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ СПП | Q.3000–Q.3999 |
| Общие аспекты | Q.3000–Q.3029 |
| Функциональные архитектуры сигнализации в сетях и управления сетями | Q.3030–Q.3099 |
| Организация сетевых данных в рамках СПП | Q.3100–Q.3129 |
| Сигнальная информация управления каналом-носителем | Q.3130–Q.3179 |
| Требования к сигнализации и управлению и протоколы для обеспечения присоединения в условиях СПП | Q.3200–Q.3249 |
| Протоколы управления ресурсами | Q.3300–Q.3369 |
| Протоколы управления услугами и сеансами | Q.3400–Q.3499 |
| Протоколы управления услугами и сеансами – дополнительные услуги | Q.3600–Q.3649 |
| Приложения СПП | Q.3700–Q.3849 |
| Тестирование для СПП | Q.3900–Q.3999 |

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Q.3309

Протокол координации QoS

Резюме

В Рекомендации МСЭ-Т Q.3309 определяется протокол координации управления допуском для СПП и дается определение интерфейсов между уровнем координации управления допуском и системами сигнализации более высокого уровня, а также между уровнем координации управления допуском и транспортными сетями нижнего уровня.

Хронологическая справка

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор* |
|---------|--------------|-------------|----------------------------|---|
| 1.0 | МСЭ-Т Q.3309 | 29.10.2009 | 11-я | 11.1002/1000/10232 |

Ключевые слова

Координация QoS, RSVP.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: <http://handle.itu.int/>, после которого следует уникальный идентификатор Рекомендации. Например, <http://handle.itu.int/11.1002/1000/11830-en>.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2018

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

| | Стр. |
|--|-------------|
| 1 Сфера применения | 1 |
| 2 Справочные документы | 1 |
| 3 Определения | 1 |
| 3.1 Термины, определенные в других документах | 1 |
| 3.2 Термины, определенные в настоящей Рекомендации | 2 |
| 4 Сокращения и акронимы | 2 |
| 5 Соглашения по терминологии | 2 |
| 6 Высокоуровневое описание | 2 |
| 6.1 Модели координации управления допуском | 3 |
| 7 Описание протокола | 4 |
| 7.1 Руководящие указания по проектированию и основы работы протокола | 4 |
| 7.2 Расширения протокола RSVP для поддержки режима координации | 6 |
| 7.3 Типы резервирования QoS | 7 |
| 7.4 Объединение | 8 |
| Дополнение I | 10 |
| I.1 Список разных типов резервирования QoS | 10 |
| I.2 Динамическое объединение | 10 |
| Библиография | 11 |

Протокол координации QoS

1 Сфера применения

В настоящей Рекомендации определяется протокол координации управления допуском. Основные проектные аспекты рассматриваемого протокола включают определение интерфейсов между уровнем координации управления допуском и системами сигнализации более высокого уровня, а также между уровнем координации управления допуском и транспортными сетями более низкого уровня. Семантика протокола также включена в определение.

ПРИМЕЧАНИЕ. – Настоящая Рекомендация является спецификацией требований к протоколу; функционально он может быть частью различных архитектур.

2 Справочные документы

В нижеследующих Рекомендациях МСЭ-Т и в других справочных документах содержатся положения, которые, с помощью ссылки в настоящем тексте, составляют положения настоящей Рекомендации. На момент публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются; поэтому всем пользователям данной Рекомендации настоятельно рекомендуется по возможности использовать последние издания перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса Рекомендации.

[IETF RFC 1633] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview*.

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP), Version 1 Functional Specification*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 Adspec [IETF RFC 2205] – сообщение Path (путь) может переносить пакет информации оповещения OPWA, известный как Adspec.

ПРИМЕЧАНИЕ. – Объект Adspec, полученный в сообщении Path, передается управлению локальным трафиком, которое возвращает обновленный объект Adspec; обновленная версия затем пересылается в сообщениях Path, передаваемых в нисходящем направлении.

3.1.2 flowspec [IETF RFC 2205] – определяет QoS, которое должно обеспечиваться для потока. Flowspec используется для установки параметров функции диспетчеризации пакетов для обеспечения запрошенного качества обслуживания. Flowspec переносится в объекте FLOWSPEC. Формат flowspec непрозрачен для RSVP и определен Рабочей группой интегральных служб IETF.

3.1.3 Rspec [IETF RFC 2205] – компонент flowspec, который определяет желаемое QoS.

ПРИМЕЧАНИЕ. – Формат Rspec непрозрачен для RSVP и определен Рабочей группой по интегральным службам IETF.

3.1.4 Tspec [IETF RFC 2205] – набор параметров трафика, которые описывают поток.

ПРИМЕЧАНИЕ. – Формат Tspec непрозрачен для RSVP и определен Рабочей группой по интегральным службам IETF.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 Пересылающий узел (forwarder) – узел, который отвечает в пределах домена за получение сквозных запросов о координации QoS, отправляет их на уровень управления допуском через интерфейс контроллера допуска, обрабатывает их и пересылает в следующий домен на сквозном пути.

3.2.2 Последний пересылающий узел (last forwarder) – пересылающий узел последнего домена на сквозном пути.

3.2.3 Инициатор запроса QoS (QoS requester) – узел, в котором функция управления сеансом или оборудование конечного пользователя запрашивают обработку QoS у сети.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | |
|--------|--|---|
| OPWA | One-Pass With Advertising | Один проход оповещения |
| QCP | QoS Coordination Protocol | Протокол координации QoS |
| RSVP | Resource ReSerVation Protocol | Протокол резервирования ресурсов |
| YESSIR | YEt another Sender Session Internet Reservations | Еще одно резервирование сеанса связи через интернет для отправителя |

5 Соглашения по терминологии

Отсутствуют.

6 Высокоуровневое описание

Для определения протокола координации управления допуском установлены четыре уровня, как показано на рисунке 6-1: уровень управления сеансом, уровень координации, уровень управления допуском и уровень применения QoS.

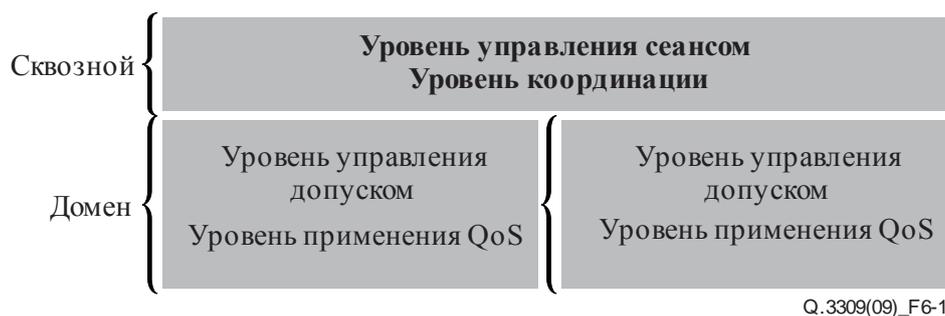


Рисунок 6-1 – Схематическое представление уровней сквозной архитектуры QoS

Уровень применения QoS реализуется в каждом домене с контролем допуска. Он передает необходимую информацию на верхний уровень управления допуском, чтобы когда уровень управления допуском примет решение о предоставлении определенной услуги потоку или пользователю, домен мог бы ее предоставить.

Уровень управления допуском реализуется в каждом домене с контролем допуска; он располагается над уровнем применения QoS и использует информацию, предоставляемую уровнем применения QoS, которая используется каждым доменом с контролем допуска для принятия решения. Его задачей является предложение интерфейса для выполнения сквозных запросов на обработку QoS. Уровень управления допуском интерпретирует эти запросы на сквозную обработку QoS и предоставляет ответ от имени всего домена, может ли запрос быть принят, а также может ли быть предоставлена запрошенная услуга.

Уровень координации располагается над уровнем управления допуском. Этот общий уровень связывает домены с контролем допуска, предоставляя набору локальных контроллеров возможность сквозного управления.

Уровень управления сеансом располагается над уровнем координации и использует его услуги для улучшения сеанса, гарантируя возможность получения определенного типа услуги из сети. Сеанс устанавливается между несколькими участниками, которые участвуют в сеансе связи. Идентификация этих участников, а также передача информации о достигнутом между всеми участниками соглашении о требованиях QoS – это две задачи этого уровня. После этого требования QoS передаются на уровень координации, который запускает механизмы создания сквозной услуги.

6.1 Модели координации управления допуском

Основным структурным элементом сети является домен с контролем допуска, который представляет собой соединение элементов сети, обеспечивающих интерфейс контроллера допуска. Объект (поток, пакет и т. п.) может запрашивать обработку QoS и получать положительный или отрицательный ответ на свой запрос. Протокол координации управления допуском действует как мост между единичным сквозным запросом и разнородными механизмами управления допуском, которые уже развернуты в сети; он предоставляет все средства для поиска, установления контакта, отправки запроса и координации ответов контроллеров допуска на всем пути. Протокол координации взаимодействует с действующим объектом, называемым демоном координации.

Существует множество способов разработки протокола координации. Это может быть:

- a) связанный или развязанный тракт. Протокол координации является связанным с трактом передачи, если он является частью тракта передачи данных, в случае развязанного тракта все наоборот; какие-либо предположения о местонахождении демона координации отсутствуют; если он тесно связан с контроллером допуска, это приведет к взаимодействию между процессами, тогда как если они будут слабо связаны, по сети будет отправлено дополнительное сообщение;
- b) без учета и с учетом предыдущего состояния относительно информации о запросах QoS. Если предыдущее состояние учитывается, демон координации хранит список всех пар объект–обработка для объектов, которые используют часть ресурсов в рамках сферы действия этого демона координации; если же предыдущее состояние не учитывается, демон координации не ведет список каких-либо объектов.

Общая схема может быть проактивной или реактивной: это применяется при наличии сбоев, повторной маршрутизации, мобильности или других исключительных событий. В этих случаях объекты могут изменить свой тракт; поэтому может потребоваться повторно выполнить действия фазы координации, а также фазы управления допуском. Если это делается проактивно, механизм координации периодически запускается, чтобы обновить состояние и отреагировать на исключительные события. В случае реактивной схемы демон координации знает об изменениях, которые приводят к исключительным событиям, и реагирует на них, повторно запуская механизм координации.

На основе такого описания можно схематически представить различные возможные архитектуры, изображенные на рисунке 6-2, где каждый овал представляет собой домен с контролем допуска; точка представляет собой интерфейс контроллера допуска, а квадрат представляет собой демон координации (следует отметить, что они могут перекрываться и создаваться в одном узле).

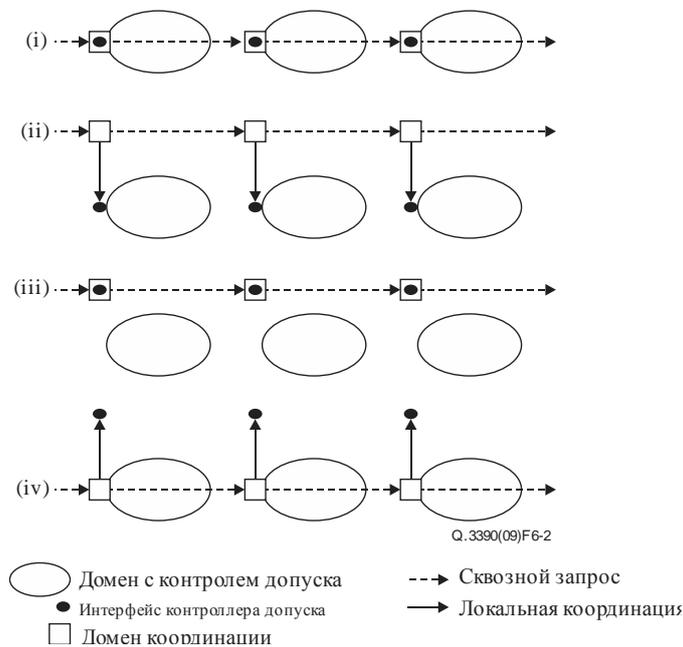


Рисунок 6-2 – Модели координации управления допуском

Среди возможных решений могут быть следующие: i) сценарий, при котором как демон координации, так и контроллер допуска связаны с трактом передачи: демон координации получает сквозной запрос, который он в свою очередь передает следующему демону координации и отправляет контроллерам допуска; ii) ситуация, при которой демон координации не связан, а контроллер допуска связан с трактом передачи; iii) сценарий, при котором как демон координации, так и контроллер допуска не связаны с трактом передачи; и, наконец, iv) решение, при котором демон координации связан, а контроллер допуска не связан с трактом передачи.

Эту модель можно дополнительно расширить, чтобы ввести понятие иерархии. Четыре представленные выше модели, в свою очередь, можно рассматривать как основные структурные элементы. Наиболее общими подходами из рисунка 6-2 являются сценарии ii) и iii). Сценарий i) совпадает со сценарием ii) при введении иерархии; сценарий iv) совпадает со сценарием ii), поскольку нельзя сделать предположения о том, сильно или слабо связаны между собой контроллер допуска и демон координации.

7 Описание протокола

В разделе 6 подробно описаны основные модели классификации координации управления допуском. В данном разделе сформулирован набор руководящих указаний по проектированию протокола координации управления допуском для интернета. Протокол RSVP расширен, чтобы сделать его подходящим для использования в качестве протокола координации управления допуском.

7.1 Руководящие указания по проектированию и основы работы протокола

Реализация такого протокола координации включает инициатор протокола, терминатор и последовательность демонов координации. При следовании от инициатора к терминатору по тракту передачи данных протокол по очереди взаимодействует с каждым демоном координации на этом пути. Допускается использование подхода как со связью, так и без связи с трактом передачи. Использование протокола RSVP означает, что нет необходимости в отдельном механизме маршрутизации. Демоны координации сначала запускают свой локальный механизм управления ресурсами (в пределах своего домена управления допуском), а затем передают результаты этого процесса, пока каждый демон координации на пути следования не представит результат своей работы. Такое взаимодействие происходит через интерфейс контроллера допуска. Протокол координации позволяет объединить разные результаты работы в один ответ инициатору запроса QoS.

7.1.1 Интерфейсы

В общем случае демон протокола может иметь до четырех интерфейсов: прикладной интерфейс, интерфейс маршрутизации, интерфейс контроллера допуска и интерфейс координации.

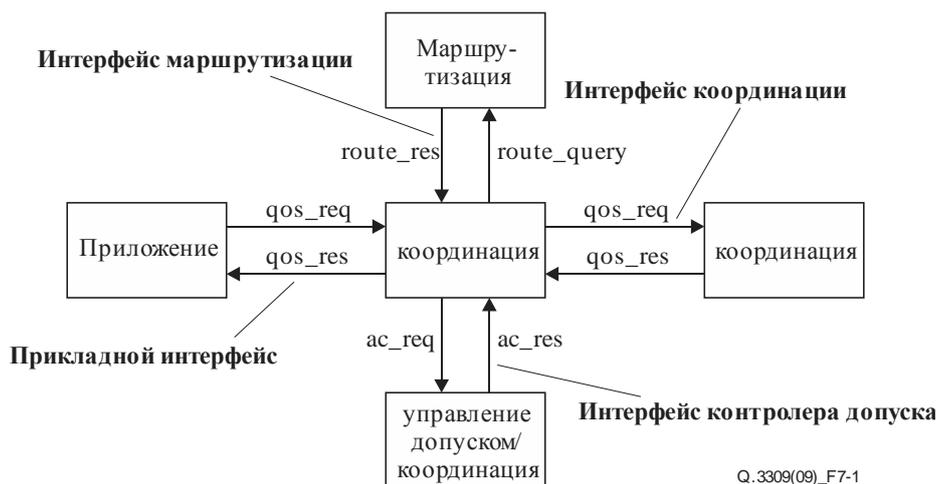


Рисунок 7-1 – Интерфейсы протокола

Интерфейс контроллера допуска вызывается функцией координации и реализуется либо другой функцией координации (то есть рекурсивно), либо функцией управления допуском. При реализации функцией управления допуском выделяются необходимые ресурсы, если таковые имеются. В случае успешного выделения ресурсов возвращается положительный результат управления допуском, тогда как при неудаче возвращается отрицательный результат.

С другой стороны, когда функция управления допуском реализуется функцией координации, интерфейс рекурсивно просматривает все функции управления допуском нижнего уровня, опрашивает их и согласует их результат в одном домене.

Интерфейс маршрутизации с помощью протокола RSVP определяет тракт для пересылки. Он также получает уведомления об изменении маршрута. Интерфейс координации используется для связи с другими демонами координации или с приложением, или с агентом вызова в конце цепочки протокола.

7.1.2 Рекурсия

Поскольку вызов интерфейса контроллера допуска выполняется прозрачно, протоколу координации неизвестен характер нижнего уровня. В частности, нижний уровень может быть протоколом, реализующим либо функцию управления допуском, либо другую функцию координации. Если реализуется функция управления допуском, то рекурсия прекращается; в противном случае при реализации дополнительной функции координации текущий домен делится дальше и координируется в рамках разделенных доменов. Этот процесс рекурсивного вызова интерфейса контроллера допуска повторяется до тех пор, пока каждый домен не настроит управление трафиком своих локальных элементов и не сообщит о результатах управления допуском. Таким образом, домен с контролем допуска может быть разделен на субдомены, где решение об управлении допуском принимается на более низком уровне. В качестве дополнительной возможности в домене или субдомене может поддерживаться исходная семантика протокола RSVP, что позволяет выполнять резервирование RSVP на маршрутизаторах, а это выходит за рамки сферы действия настоящей Рекомендации.

7.1.3 Семантика протокола

Если протокол координации имеет свойства, описанные в предыдущих разделах, то семантика обмена сообщениями аналогична семантике протоколов резервирования ресурсов, таких как RSVP [IETF RFC 1633] и YESSIR. Поддерживаются две модели:

- двухэтапная модель предоставления или резервирования ресурсов – демон координации получает запрос QoS, который передается системе управления ресурсами в целях резервирования ресурсов без их предоставления;
- одноэтапная модель предоставления ресурсов – демон координации получает запрос QoS, который передается системе управления ресурсами в целях предоставления ресурсов.

Разница между этими двумя вариантами заключается в том, когда именно ресурсы предоставляются, то есть когда принимается решение об управлении допуском. Учитывая это, данный протокол может работать двумя способами в зависимости от того, находится ли запрос QoS в режиме блокировки (отсутствия блокировки) для демона координации.

- Режим блокировки – демон координации передает системе управления ресурсами запрос на предоставление ресурсов, ожидает ответ, а затем переправляет дальше как запрос на предоставление ресурсов, так и ответ на него.
- Режим отсутствия блокировки – демон координации передает системе управления ресурсами запрос на предоставление ресурсов, переправляет запрос предоставления ресурсов дальше и ожидает получения ответа в восходящем направлении.

7.2 Расширения протокола RSVP для поддержки режима координации

Протокол RSVP [IETF RFC 2205] обеспечивает сигнализацию QoS для потоков данных приложений. Инициаторы запроса QoS могут использовать протокол RSVP для запроса у сети определенных уровней качества обслуживания (QoS) для потоков данных конкретных приложений. Домен управления допуском использует протокол RSVP для доставки запросов QoS на все узлы на маршруте передачи данных. Протокол RSVP также может поддерживать и обновлять состояния для запрошенного уровня качества обслуживания (QoS) потока приложения.

Структура RSVP имеет ряд существенных отличий, среди которых управление гибким состоянием, двухэтапный обмен сообщениями резервирования или предоставления ресурсов, а также отделение сигнализации от маршрутизации.

Протокол RSVP обеспечивает передачу сообщений сигнализации QoS по сети, посещая каждый узел на маршруте передачи данных, используя обычную маршрутизацию IP. Для резервирования ресурсов на узле демон RSVP взаимодействует с двумя локальными модулями принятия решений – модулем управления допуском и модулем управления политикой. Модуль управления допуском определяет, имеются ли на узле ресурсы, достаточные для предоставления запрошенного уровня качества обслуживания (QoS). Модуль управления политикой обеспечивает авторизацию запроса QoS. Если какая-либо из проверок заканчивается неудачей, модуль RSVP возвращает уведомление об ошибке прикладному процессу, который является источником запроса. Если обе проверки проходят успешно, модуль RSVP устанавливает параметры в классификаторе пакетов и в планировщике пакетов для получения необходимого уровня качества обслуживания (QoS).

RSVP подходит для поддержки координации управления допуском, поскольку обладает большинством свойств, которые необходимы протоколу координации QoS:

- 1) RSVP может быть связан с маршрутом; и
- 2) может использоваться рекурсивно.

Тем не менее имеется ряд существенных характеристик, не свойственных RSVP, в том числе:

- осведомленность о домене – RSVP не осведомлен о домене;
- интерфейс контроллера допуска – демоны RSVP поддерживают интерфейс контроллера допуска. Хотя пока используется режим координации, этот интерфейс, вероятно, будет другим и более общим;
- семантика протокола – обмен сообщениями RSVP основан на двухэтапной модели резервирования или предоставления ресурсов. Для поддержки режима координации необходима одноэтапная модель обмена;

- поле режима – RSVP должен поддерживать поле заголовка сообщения, чтобы была возможность отличать его использование в режиме резервирования от его использования в режиме координации. Домен с контролем допуска может использовать расширенный RSVP, обрабатывая режим координации так же, как и режим резервирования. Домен самостоятельно выберет необходимый вариант;
- поле рекурсии – RSVP может быть использован рекурсивно; однако у него нет явного поля заголовка сообщения, которое бы явно указывало на уровень рекурсии. Оно будет необходимо для обработки рекурсивных протоколов;
- предварительное бронирование QoS – это запрос QoS для использования в будущем, а не для немедленного использования. RSVP не поддерживает предварительное бронирование QoS;
- инициирование отправителем – RSVP иницируется получателем. Необходима возможность инициирования отправителем, а также возможность инициирования с помощью прокси-отправителя или получателя.

Расширенная версия RSVP объединяет функции резервирования ресурсов и координации. Когда используется режим резервирования, RSVP работает в обычном порядке. Когда используется режим координации, RSVP работает следующим образом. Обмен сообщениями задействует один узел для каждого домена управления допуском, то есть данные проходят через каждый входной узел. После получения запроса входной узел иницирует свой локальный механизм управления ресурсами и пересылает этот запрос на следующий входной узел на маршруте передачи данных. Этот процесс повторяется до тех пор, пока запрос не достигнет терминатора. Терминатор выдает ответ, который проходит через все те же входящие узлы, собирая и объединяя результаты различных процессов управления допуском (успех/отказ). Дошедший до инициатора ответ будет содержать все данные, полученные на пути от инициатора к терминатору, включая ответ управления допуском.

Входные узлы представляют собой для этого домена точку контакта по умолчанию, на которой работает копия протокола координации управления доступом. Когда нет необходимости в том, чтобы контроллер допуска представлял собой точку контакта по умолчанию для этого домена, демон координации пересылает (через интерфейс контроллера допуска) этот запрос к соответствующему объекту, настроенному локально.

7.3 Типы резервирования QoS

Существуют разные возможные виды семантики резервирования: однопроходный механизм (предоставление ресурсов/ошибка), двухпроходный механизм (резервирование/предоставление ресурсов) и однопроходный с оповещением (OPWA). Для типа резервирования OPWA сообщения оповещения от инициатора запроса QoS поступают на каждый интерфейс контроллера допуска в доменах на сквозном пути. Когда они достигают получателя, в них содержатся все показатели Rspec, что приводит к резервированию соответствующего объекта (определенного по его Tspec) для разных типов услуг, которые может предоставить сеть. Затем на основе выбора среди всех разнообразных услуг и информированности о всех показателях Rspec может быть принято соответствующее решение.

В настоящей Рекомендации используется OPWA, поскольку это метод обеспечивает полную гибкость. Рекомендуется, чтобы протокол координации QoS содержал третий поток сообщений для обработки ситуации в тех случаях, когда на конечной точке доступно оповещение об услугах сети (наиболее вероятно получателю), при этом конечная точка не является точкой принятия решения о выборе услуги. В таком случае рекомендуется установить связь с объектом, который отвечает за принятие решения, и предоставить ему информацию о различных услугах, а также задать вопрос о том, какую услугу следует выбрать.



Рисунок 7-2 – Сценарий одного прохода с оповещением (OPWA)

Схематическое представление описанного выше сценария показано на рисунке 7-2.

- 1) Отправитель связывается с наложенной сигнализацией сеанса, которая различает участников и согласовывает тип носителя.
- 2) Элемент управления сеансом инициирует механизмы координации QoS через прикладной интерфейс (как показано на рисунке 7-1), связываясь с инициатором запроса QoS.
- 3) Если в качестве протокола сигнализации принимается RSVP, инициатор запроса QoS отправляет сообщение PATH в нисходящем канале (которое проходит через все элементы управления допуском посредством интерфейсов контроллера допуска) с указанным значением Tspec потока. Сообщение PATH собирает данные оповещения в объекте ADSPEC; полный Adspec присутствует в последнем пересылающем узле (то есть интерфейсе контроллера допуска).
- 4) Информация Adspec затем отправляется назад к инициатору запроса QoS (при условии, что инициатор запроса QoS подходит для принятия решений).
- 5) Инициатор запроса QoS принимает решение и отправляет его последнему пересылающему узлу.
- 6) Последний пересылающий узел может затем отправить назад сообщение RESV, чтобы зарезервировать конкретный ресурс для выбранной услуги.

7.4 Объединение

Модель координации, представленная в разделе 6, явно предназначена для каждого потока и требует сквозного соглашения об обработке. Из этого следует необходимость планирования обмена отдельными сообщениями для каждого запроса.

Объединение является одним из способов сокращения количества сообщений, объема хранимой информации и времени обработки для уровня координации, когда таких задач становится слишком много во внутренних доменах сети. Как правило, объединение предполагает, что в крайних точках (то есть где возможна обработка отдельного потока QoS) предпринимаются усилия для объединения потоков, с тем чтобы они совместно использовали общий путь в своей основе и выполняли аналогичные требования QoS. Вследствие этого они обрабатываются вместе, что снижает затраты на индивидуальную обработку без уменьшения эффективности получения услуг.

В общем случае можно определить два разных подхода к установлению границ зоны объединения – статическое объединение и динамическое объединение.

Объединение является статическим, когда зона объединения определяется таким образом, что в пределах ее границ потоки обрабатываются как объединенные. При таком решении границы области

действия домена определяются администраторами сети так, чтобы получить максимальную пользу от процесса объединения. Такое решение может быть осложнено наличием нескольких доменов.

Динамическое объединение используется динамически в зависимости от различных факторов, таких как направление потока, количество потоков, а также положение в сети доменов, обрабатывающих определенный поток. Динамическое объединение выходит за рамки сферы применения настоящей Рекомендации, поскольку его сложно реализовать на практике.

7.4.1 Метод маркировки

В том случае, когда в качестве метода туннелирования используется MPLS, можно применять разные тракты с коммутацией по меткам, чтобы при обработке QoS различать разные потоки, которые проходят по одному объединенному тракту. Для обеспечения мультиплексирования различных функций обработки QoS в границах всей совокупности используется второй вложенный заголовок. Например, для объединенного трафика может использоваться заголовок UDP, который совместим с классификацией пакетов FILTER_SPEC; поле порта источника UDP может использоваться для объединения разной обработки пакетов, порт UDP получателя может использоваться для других целей. Это можно увидеть на рисунке 7-3.

| | | | |
|------------------------|-------------------------|--------------|----------------------------|
| Вложенный заголовок IP | Вложенный заголовок UDP | Заголовок IP | Пакет транспортного уровня |
|------------------------|-------------------------|--------------|----------------------------|

Q.3309(09)_F7-3

Рисунок 7-3 – Пакеты для объединенного трафика

Дополнение I

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Список разных типов резервирования QoS

В таблице I.1 приводится пояснение разных типов резервирования QoS, позволяющее лучше понять информацию, представленную в разделе 7.3.

Таблица I.1 – Типы резервирования QoS

| Типы резервирования QoS | Определения |
|---|--|
| Однопроходный механизм (предоставление ресурсов или ошибка) | От отправителя запросы на резервирование поступают на каждый интерфейс контроллера допуска в доменах на всем сквозном пути. Резервирование либо допускается – при этом процесс продолжается, либо нет – при этом по восходящему направлению распространяется каскад ошибок, чтобы отменить уже предоставленное резервирование. Однако при таком сценарии для уровня координации нет разумного способа получить в конце пути резервирования такие, например, показатели, как сквозная задержка или границы дрожания; следовательно, с помощью этого механизма уровень координации может только уведомлять все домены о том, какую услугу желательно получить от каждого домена |
| Двухпроходный механизм (резервирование – предоставление ресурсов) | От отправителя запросы на резервирование поступают на каждый интерфейс контроллера допуска в доменах на всем сквозном пути за два прохода. При первом проходе отправитель вставляет Rspec, сеть резервирует услугу, которая соответствует запросу с самыми близкими показателями. На стороне получателя принимается информация о глобальном резервировании; если характеристики услуги, которую может предоставить сеть, ниже требуемых, резервирование отклоняется и аннулируется; если они даже выше требуемых, то характеристики услуги могут быть снижены, при этом будет содержаться информация об избыточных ресурсах. Этот сценарий допускает спецификацию всех показателей Rspec |
| Один проход с оповещением (OPWA) | См. раздел 7.3 |

I.2 Динамическое объединение

Динамическое объединение используется динамически в зависимости от различных факторов, таких как направление потока, количество потоков, а также положение доменов, обрабатывающих определенный поток, в сети. Создание зоны динамического объединения не является простой задачей и может быть выполнено в результате координации локальных решений доменов с контролем допуска. Каждый домен на пути передачи определяет, следует ли использовать объединение на основе локальных политик. В результате этого с помощью уровня координации происходит обмен локальными решениями, при этом выполняется динамическое построение зон объединения. Это не создает проблем, когда все происходит внутри домена, но может привести к сложностям при междоменном взаимодействии между соседними узлами, когда может быть доступно меньше информации. Кроме того, такой подход может привести к обмену большим количеством сообщений и большим затратам на вычисления, связанным с обменом локальными решениями и координацией разных доменов.

Библиография

- [b-ITU-T H.360] Рекомендация МСЭ-Т H.360 (2004 год), *Архитектура для сквозного управления и сигнализации QoS*
- [b-ETSI RACS] ETSI RACS Release 1 (2005), *NGN functional architecture; Resource and Admission Control Subsystem (RACS)*
- [b-IETF RFC 2638] IETF RFC 2638 (1999), *A Two-bit Differentiated Services Architecture for the Internet*
- [b-IETF RFC 2702] IETF RFC 2702 (1999), *Requirements for Traffic Engineering Over MPLS*
- [b-IETF RFC 2814] IETF RFC 2814 (2000), *A Protocol for RSVP-based Admission Control over IEEE 802-style networks*
- [b-IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*
- [b-IETF WG Charter] IETF WG Charter (1996), *Integrated Services over Specific Link Layers, IETF Working Group charter.*
<<http://www.ietf.org/proceedings/37/charters/issll-charter.html>>
- [b-IETF WG Charter 1] IETF WG Charter (2009), *Next Steps In Signalling, IETF Working Group charter.*
<<http://www.ietf.org/html.charters/nsis-charter.html>>
- [b-3GPP TR23.802] 3GPP TR23.802 (2007), *Architectural enhancements for end-to-end Quality of Service*
- [b-ACM Tussle] ACM SIGCOMM Tussle in Cyberspace (2002), *Tussle in Cyberspace: Defining Tomorrow's Internet*
- [b-ATM forum TM V4.0] The ATM Forum Technical Committee (1996), *Traffic Management Specification Version 4.0*
- [b-BTTJSE Guaranteed QoS synthesis] Hovell, P., Briscoe, R., Corliano, G. (2005), *Guaranteed QoS synthesis – An example of a scalable core IP quality of service solution*, British Telecommunications Technical Journal Special Edition on IP Quality of Service
- [b-IFIP TC6 EuQoS] IFIP TC6 Conference EuQoS (2005), *End to End Quality of Service over Heterogeneous Networks (EuQoS), In Proc. Network Control and Engineering for QoS, Security and Mobility, IFIP TC6 Conference, NetCon'05, Lannion, France*
- [b-MSF-TR-ARCH-005-FINAL] Gallon, C., Schelén, O. (2005), *Bandwidth management in next generation packet networks, MSF Technical Report ARCH-005-FINAL*
- [b-PacketCable 050812] pkt-sp-dqos-I12-050812 (1999), *PacketCable Dynamic Quality of Service Specification*

[b-QBBB]

QBBB, Internet2 Bandwidth Broker Working Group,
QBone Bandwidth Broker Architecture.
<<http://qbone.internet2.edu/bb/>>

[b-YESSIR]

YESSIR (1999), *YESSIR: A Simple Reservation
Mechanism for the Internet*, Computer Communication
Review, vol. 29

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|----------------|---|
| Серия А | Организация работы МСЭ-Т |
| Серия D | Общие принципы тарификации |
| Серия E | Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы |
| Серия F | Нетелефонные службы электросвязи |
| Серия G | Системы и среда передачи, цифровые системы и сети |
| Серия H | Аудиовизуальные и мультимедийные системы |
| Серия I | Цифровая сеть с интеграцией служб |
| Серия J | Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов |
| Серия K | Защита от помех |
| Серия L | Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений |
| Серия M | Управление электросвязью, включая СУЭ и техническое обслуживание сетей |
| Серия N | Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ |
| Серия O | Требования к измерительной аппаратуре |
| Серия P | Оконечное оборудование, субъективные и объективные методы оценки |
| Серия Q | Коммутация и сигнализация |
| Серия R | Телеграфная передача |
| Серия S | Оконечное оборудование для телеграфных служб |
| Серия T | Оконечное оборудование для телематических служб |
| Серия U | Телеграфная коммутация |
| Серия V | Передача данных по телефонной сети |
| Серия X | Сети передачи данных, взаимосвязь открытых систем и безопасность |
| Серия Y | Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений |
| Серия Z | Языки и общие аспекты программного обеспечения для систем электросвязи |